Information Security Policy

This policy aims to establish guidelines and procedures to promote the protection of Continental Parafusos' assets, ensuring their confidentiality, integrity, and availability. Additionally, it seeks to meet applicable regulatory and normative requirements, while promoting an information security culture within the organization. The policy is directly linked to:

- IT (Information Technology)
- ISMS (Information Security Management System)
- LGPD (General Data Protection Law)

The policy includes guidelines for protecting both physical and logical information assets, promoting:

- **Availability**: by ensuring information is accessible when needed;
- **Integrity**: by preserving the consistency and reliability of information and systems;
- **Confidentiality**: by protecting information from unauthorized disclosure.

These guidelines must be followed by all employees, service providers, business partners, and any individual or entity with access to Continental Parafusos information.

Non-compliance with Continental Parafusos' security policies may result in administrative and legal sanctions, depending on the severity of the violation:

- **Administrative Measures**: Warnings, suspensions, and restricted access to systems for those who breach security guidelines.
- **Legal Actions**: Severe violations, such as misuse of data or intentional compromise of systems, may lead to legal proceedings and contract termination.
- **Sanction Enforcement**: Penalties will be proportional to the severity of the incident and in accordance with the LGPD and current labor laws, ensuring the protection of the company's assets.

Information Classification:

- **Confidential Information:** Must be kept strictly confidential to avoid financial losses, reputational damage, or loss of competitiveness. Its exposure outside the organization may result in serious harm.
- **Restricted Information:** Limited to a specific group of users responsible for its creation or processing. It is shared internally and, when necessary, externally. It has a medium level of confidentiality.
- **Internal Information:** Intended for internal knowledge within the organization.
- **Public Information:** May be disclosed to everyone, including employees, contractors, customers, suppliers, and the general public, without causing negative business impacts.

Who is the ISMS intended for?

All employees, service providers, and partners of Continental Parafusos must follow the standards and best practices described in this policy. It is the responsibility of each person to ensure the protection of information and to encourage others to do the same, fostering a culture of information security within the company.

The responsibilities regarding Information Security are as follows:

- **Top Management:** Provides resources for the improvement of information security management.
- **Committee:** Requests resources from Top Management and approves the Information Security Policy (ISP).
- **Information Technology and Security Officer:** Implements, monitors, and reviews the ISMS, proposes improvements, and leads asset and risk mapping.
- **Information Technology and Security Team:** Conducts training, access control, incident response, and backup monitoring.
- **Area Leaders:** Ensure their teams are aware of and comply with the ISP, and collaborate with IT in access reviews and incident reporting.

- **Employees, Interns, Third Parties, and Suppliers / service providers:** Must protect information, follow the ISP, and report any incident to the IT Officer.

Key Concepts and Definitions in This Process:

- **Asset:** Any element that adds value to the business, which may include digital or physical information, hardware, software, people, or physical environments.
- **Information Asset:** Business-critical information that must be protected.
- **Supporting Assets:** Resources associated with information and its processing, such as hardware, software, IT systems, and employees.
- **Information Security:** The protection of the organization's assets against various threats.
- **Information Security Incident:** An event or series of events that impact the availability, integrity, or confidentiality of an information asset.

Information Security Incident Handling:

To ensure an appropriate response to information security incidents, Continental Parafusos establishes guidelines for their detection, analysis, response, containment, recovery, and documentation. Incidents may compromise the confidentiality, integrity, or availability of information and must be addressed with appropriate urgency based on their criticality.

Response Guidelines

After an incident is reported, the Information Technology and Security Team must:

- Assess the severity and classify the incident;
- Act in accordance with the defined SLA (Service Level Agreement), ranging from 3 to 16 hours;
- Document all evidence;
- Perform containment and recovery actions, such as using backups and temporarily suspending access;
- Notify relevant stakeholders and ensure traceability of records;
- Conduct a semiannual critical analysis of recorded incidents to support preventive actions and continuous improvement.

Communication Channels:

Incident Notification and Reporting

Incident Type	Notification / Reporting Channel	Reason	Department Responsible for Management
Information Technology	**Internal reports:** GLPI Ticketing System **External reports:** - E-mail: gestao.ti@continentalparafusos.com.br or - Telephone: +55 11 4043-4144 – Internal extension 1086	System failures, unauthorized access, intrusion attempts, phishing, malware, ransomware, etc.	Information Technology and Information Security, and the party responsible for IT and IS
Personal Data	- E-mail: privacidade_lgpd@continentalparafusos.com.br - Telephone: +55 11 4043-4144 – Internal extension 1040	Leakage, loss, unauthorized use, or improper sharing of personal data	LGPD Officer (Data Protection Officer)
Leakage of Verbal Information or Physical Documents	- Open Door HR – Suggestion Box - Directly to HR or immediate manager – by e-mail or in person	Confidential information discussed in public places, printed documents without proper control, improper disposal, etc.	Human Resources or Manager, with support from Human Resources
Physical Security	- Gatehouse / Security – 24-hour service - Internal extension 1068 - Or telephone: +55 11 4043-4144 - Headquarters: +55 11 96186-6893 – G9 +55 11 99552-5804	Theft, damage to property, unauthorized access, suspicious movement in restricted areas	Industrial Engineering / Party responsible for IT and IS and/or Human Resources
Other Occurrences and Operational Emergencies	**24-hour service channel:** +55 11 4043-4144 or - Headquarters: +55 11 96186-6893 – G9 +55 11 99552-5804	Work accidents, fires, threats to physical integrity, harassment, or inappropriate behavior	Industrial Security and Information Security / Human Resources

Access to the Full Policy

To obtain the complete version of Continental Parafusos' Information Security Policy, please submit a formal request through the official channel:

- ti@continentalparafusos.com.br

The request will be evaluated by the responsible team, considering the justification provided and the necessity of access to the document. The full policy will be shared upon approval, in accordance with confidentiality criteria, purpose, and appropriate use.

Information security is everyone's responsibility!
Help protect data and share this knowledge with the entire Continental Parafusos team.

CONTINENTAL PARAFUSOS S.A.